Mise en conformité RGPD : Mode d’emploi

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
					

Mettre un établissement en conformité avec le RGPD nécessite la réalisation de certaines tâches plus techniques et organisationnelles que juridiques, même si ce dernier domaine doit aussi être maîtrisé par le DPO (Data Protection Officer).

Une mise en conformité nécessitera donc une excellente connaissance en matière de sécurité informatique, d'analyse de risques, d'organisation des services, de transferts de flux de données et enfin de pédagogie pour que l'ensemble des employés de l'établissement comprenne le but de la démarche pour devenir acteur.

Les étapes à respecter sont :

1. Établir une cartographie de l'ensemble des traitements de données de l'entreprise ou de l'entité publique ;
2. Vérifier les spécificités et dispenses propres à l'activité ou au statut de l'établissement ;
3. Analyser chaque traitement de données en profondeur pour vérifier sa conformité avec le règlement ;
4. Tenir un registre dans lequel seront référencés les différents traitements des données à caractère personnel conformes et à modifier ;
5. Tenir compte de l'évolution de l'entreprise et s'assurer que la conformité est maintenue dans le temps.

Ne pas oublier que le RGPD prévoit l'obligation de déclarer une faille, entraînant une fuite ou un vol de données personnelles, auprès de l'autorité de contrôle dans les 72 heures suivant l'incident. Le DPO pourra accompagner l'établissement dans la gestion de ces incidents.
Enfin, le DPO devra traiter les demandes d'accès à ses données personnelles, formulées par exemple par un client.

Le DPO obligatoire pour qui ?

Le Règlement général sur la protection des données (RGPD), qui sera effectif le 25 mai 2018, rend obligatoire la nomination d'un Data Protection Officer (DPO) pour les entités publiques et certaines entreprises. « *Ce délégué à la protection des données sera au cœur du nouveau cadre juridique européen »,* résume le groupe de travail G29, qui réunit les « Cnil européennes ». La nomination d'un DPO sera donc incontournable pour toutes les entités publiques du Vieux Continent, telles que les collectivités locales, les hôpitaux, les universités… Côté entreprises, le DPO sera obligatoire pour celles dont l'activité principale les amènent à réaliser à grande échelle un suivi régulier et systématique des personnes (profiling), ou de traiter des données «sensibles» – santé, opinions politiques ou religieuses, orientation sexuelle, etc. – ou des données relatives à des condamnations et infractions pénales.

Parmi les entreprises qui devraient être concernées par cette obligation : des sociétés d'e-commerce ou de marketing digital, des banques et assurances, des établissements de soins ou encore des entreprises du secteur des télécoms.

« *Même lorsque le RGPD n'exige pas spécifiquement la nomination d'un DPO, les entreprises pourront parfois estimer utile d'en désigner un sur une base volontaire* », poursuit le G29. Car en effet, le nouveau règlement européen renforce très sensiblement les responsabilités des entreprises en matière de protection des données personnelles et surtout les sanctions. En France, le plafond maximal des sanctions de la Cnil est déjà passé de 150000 euros à 3 millions d'euros avec la Loi pour une république numérique de 2016. Les amendes prévues par le RGPD peuvent quant à elles atteindre 20 millions d'euros ou 4% du chiffre d'affaires mondial. De quoi inciter de nombreuses entreprises à nommer un DPO pour s'assurer de leur conformité avec le nouveau règlement.

Le DPO comment ?

Le premier travail d'un DPO sera d'établir une cartographie de l'ensemble des traitements de données de l'entreprise ou de l'entité publique. Pour cela, le DPO devra se rapprocher des représentants des différentes instances de l'organisation pour rassembler les informations nécessaires. Une fois cette cartographie réalisée, le DPO analysera chaque traitement de données en profondeur pour vérifier sa conformité avec le règlement.

Le DPO combien ?

Il n'existe pas encore de grille salariale établie pour le DPO, ses revenus devraient être au moins comparables à ceux du CIL, soit environ 50000 euros par an. La pénurie attendue de candidats au poste de DPO devrait même tirer les salaires vers haut. La Cnil prévoit que plus de 80000 organisations, publiques ou privés, devront se doter d'un DPO en France.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Source : Denis JACOPINI et *Data Protection Officer : un gardien pour les données personnelles*

Faille de sécurité dans des caméras de vidéosurveillance FLIR

	Faille de sécurité dans des caméras de vidéosurveillance FLIR

Un chercheur en sécurité informatique découvre comment accéder aux images de caméras de vidéosurveillance thermiques FLIR.

Infiltration possible dans des caméras de vidéosurveillance ! Étonnante révélation, fin septembre, par un internaute du nom de LiquidWorm. Ce chercheur en sécurité informatique a diffusé un code qui permet de découvrir que les caméras thermiques de vidéo surveillance de marque FLIR pouvaient être espionnées. FLIR Systems a des identifiants de connexion SSH codés en dur dans sa version distribuée sous Linux.

Bref, un accès aux images, via cet accès caché qui ne peut être modifié !

Cette backdoor est dénoncée quelques jours avant le salon Milipol qui se déroulera en novembre à Paris. Flir Systems y sera présent pour présenter son matériel.

Selon l'information diffusée par « Zero science« , les modèles de caméras incriminées sont les 10.0.2.43 (logiciel F/FC/PT/D) et les versions du micrologiciel 8.0.0.64: □□1.4.1, 1.4, 1.3.4 GA, 1.3.3 GA et 1.3.2 sont concernés par cette porte cachée…[lire la suite]

Réagissez à cet article

Source : *ZATAZ Une porte cachée dans des caméras de vidéosurveillance FLIR – ZATAZ*

Les nouvelles techniques des pirates pour piller les distributeurs de billets

	Les nouvelles techniques des pirates pour piller les distributeurs de billets

Phishing, hacking, infections « fileless », prise de contrôle à distance… Les braqueurs de banque utilisent des méthodes de plus en plus sophistiquées, presque invisibles, pour mettre la main sur le pactole des banques.

Quand on pense à des braqueurs de banque, on s'imagine la plupart du temps une bande de malfrats cagoulés et armés jusqu'aux dents, fonçant sur les agences en voiture-bélier. Mais la réalité est bien différente de nos jours. C'est souvent à coup d'ordinateurs et de codes malveillants que les braqueurs du XXIe siècle mettent la main sur le liquide des distributeurs, et cela avec un degré de technicité de plus en plus impressionnant.

D'après un rapport que vient de publier l'agence Europol, les premiers malwares qui ont permis de vider des guichets automatiques datent de 2009. Ils s'appellent Skimer, Ploutus ou Padkin-Tyupkin, et nécessitent d'accéder physiquement à l'intérieur de ces machines. Pour cela, les pirates s'appuient soit sur un complice de la banque, soit sur un jeu de clés. En effet, il arrive que les distributeurs ne soient protégés qu'avec de simples verrous de type boîte aux lettres !

A l'intérieur du distributeur se trouve généralement un PC sous Windows XP que les pirates infectent avec une porte dérobée. Celle-ci est installée directement depuis un CD ou une clé USB au niveau de XFS (Extension for Financial Services), un *middleware* qui permet de gérer l'interaction entre les différents éléments logiciels et matériels du distributeur: clavier, lecteur de carte, cassettes d'argent, processeur de chiffrement, etc.

Des mules pour récupérer le magot

L'infection nécessite habituellement un démarrage sous Linux. Puis les pirates repassent la machine sous Windows XP et referment les ouvertures physiques. Toute cette opération prend moins de 10 minutes. En apparence, tout fonctionne de nouveau comme avant. En réalité, la porte dérobée permet à des mules d'entrer des commandes secrètes par le clavier numérique et d'éjecter l'argent. Voici une démonstration réalisée en 2014 par les chercheurs de GData…[lire la suite]

http://www.youtube.com/embed/rZ8_tbTnNUE

Réagissez à cet article

Source : *Les nouvelles techniques des pirates pour piller les distributeurs de billets*

Télétravail : gare aux failles de sécurité

Télétravail : gare aux failles de sécurité

Le télétravail fait entrer dans les systèmes d'information de l'entreprise des appareils dont le niveau de sécurité peut s'avérer à risque.

Les directeurs des systèmes d'information (DSI) s'arrachent déjà les cheveux. Si nombre de métiers, comme ceux des commerciaux ou des consultants, sont déjà équipés pour travailler à distance en toute sécurité, le télétravail pousse hors des murs de l'entreprise des salariés souvent peu sensibilisés aux risques de cybersécurité.

D'une part, travailler de chez soi pose la question de la sécurité du matériel. La connexion Internet est-elle sécurisée ? Le chiffrement du disque dur en cas de perte est-il actif ? L'identification par SMS ou par token est-elle en vigueur ? « *Autant de questions auxquelles les DSI doivent répondre pour sécuriser le travail à distance. Les mesures sont simples et souvent déjà déployées pour certains salariés mais il faut désormais les généraliser* »…[lire la suite]

Réagissez à cet article

Source : *Télétravail : gare aux failles de sécurité, Cybersécurité – Les Echos Business*

20% des ordinateurs de la Police de Manchester son sous Windows XP

	20% des ordinateurs de la Police de Manchester son sous Windows XP

GREATER MANCHESTER POLICE are still using defunct operating system Windows XP on one-in-five machines in active use on the force.

The second biggest police force in the UK joins the Metropolitan Police on the list of shame, according to new findings from a Freedom of Information Act request made by*the BBC.*

« The remaining XP machines are still in place due to complex technical requirements from a small number of externally provided highly specialised applications, » a spokeswoman told Auntie Beeb.

« Work is well advanced to mitigate each of these special requirements within this calendar year, typically through the replacement or removal of the software applications in question. »

Most forces refused to cooperate with the FOI request, citing security reasons. This includes the Met Police who back in June admitted they had 18,000 machines that still run XP (including offline ones) and that only eight machines were running Windows 10…[lire la suite]

Réagissez à cet article

Source : *Manchester Police are using Windows XP on one in five computers*

Alerte : CCleaner compromis par une backdoor

	Alerte : L’utilitaire CCleaner compromis par une backdoor

Piriform avertit que son logiciel CCleaner a été compromis. Avec des risques de fuites de données persos de 130 millions d'utilisateurs.

Piriform, l'éditeur de l'utilitaire CCleaner de nettoyage et d'optimisation de Windows, vient de reconnaître qu'il a fait l'objet d'une attaque.

Les versions 5.33.6162 sur poste fixe et 1.07.3191 en mode Cloud de sa solution ont été compromises.

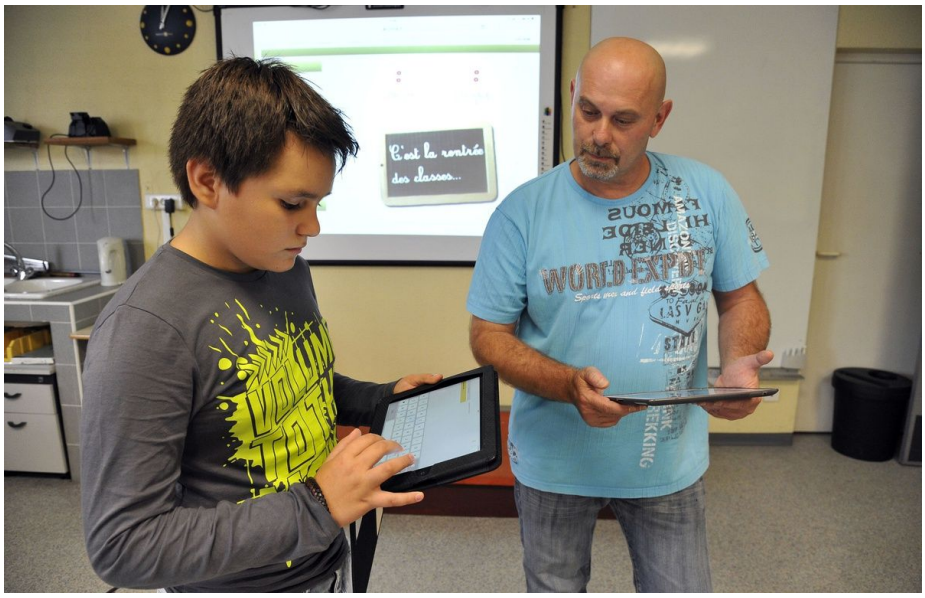
« Une activité suspecte a été identifiée le 12 septembre 2017, où nous avons vu une adresse IP inconnue recevant des données du logiciel trouvé dans CCleaner et CCleaner Cloud sur les systèmes Windows 32 bits », alerte Paul Yung, Vice-Président Produit de Piriform.

Selon l'éditeur, le logiciel a été illégalement modifié avant sa livraison publique. Le pirate a réussi à installer une backdoor à deux niveaux afin d'exécuter du code envoyé à partir d'une adresse IP sur les systèmes affectés…[lire la suite]

Réagissez à cet article

Source : *L'utilitaire CCleaner compromis par une backdoor*

Les données personnelles des écoliers français vont-elles échapper à Google?



Les données personnelles des écoliers français vont-elles échapper à Google?

Une «note interne» diffusée en mai ouvrait la possibilité aux entreprises du numérique de collecter des données scolaires. Les parents d'élèves avaient protesté auprès du ministre de l'Education. Jean-Michel Blanquer compte revoir la politique en la matière.

Pas d'école pour Google, Facebook, et autres géants du numérique, regroupés sous l'appellation Gafa. Jeudi, le porte-parole du gouvernement a indiqué que le ministre de l'Education Jean-Michel Blanquer comptait limiter l'accès de ces entreprises aux données scolaires des élèves.

Le ministre compte « revenir sur une circulaire [en fait, une lettre interne] signée deux semaines avant les présidentielles, qui ouvre très largement, peut-être trop largement l'accès des Gafa dans l'école », a expliqué Christophe Castaner.

Publicités ciblées

Rappel des faits : le 12 mai dernier, Matthieu Jeandron, délégué au numérique éducatif, adresse une lettre aux délégués académiques du numérique. Dans ce courrier, révélé par le Café pédagogique, il explique qu'il n'y a pas « de réserve générale sur l'usage des outils liés aux environnements professionnels chez les grands fournisseurs de service du web ». Un peu plus loin, il indique qu'il ne voit pas de « blocage juridique de principe à la connexion d'un annuaire avec l'un de ses services ».

En clair, cela signifie que Google, Facebook, et autres entreprises du numérique auraient pu collecter des listes d'élèves avec leurs noms, leurs classes, voire même leurs notes dans le cadre de travaux effectués en ligne. Ces données peuvent rapporter de l'argent : par exemple, on peut imaginer que Google, ayant connaissance des difficultés d'un élève, lui « propose » des publicités ciblées sur les cours en lign…[lire la suite]

Réagissez à cet article

Source : *Les données personnelles des écoliers français vont-elles échapper à Google?*

Comment pirater un téléphone sans le toucher ?

L'exploitation de failles de sécurité se trouvant au niveau du protocole Bluetooth permet de pirater un appareil à distance. La démonstration est faite sur un smartphone Android, mais les vulnérabilités concernent potentiellement d'autres types d'appareils.

Armis, entreprise spécialiste des questions de sécurité informatique, a découvert huit exploits (ces éléments de programme visant à exploiter une faille informatique) réunis sous l'étiquette BlueBorne, et permettant de prendre à distance le contrôle de téléphones, d'objets connectés et même potentiellement d'ordinateurs. *« Nous nous attendons à découvrir beaucoup d'autres vulnérabilités de ce type sur diverses plateformes proposant une connexion Bluetooth. Ces failles sont actuellement ouvertes, et peuvent être exploitées par les hackers. Les attaques via BlueBorne peuvent être utilisées pour réaliser tout un arsenal de piratages différents, autorisant l'exécution de code malveillant à distance ou encore la prise de contrôle des appareils*« , explique Armis….[lire la suite]

Réagissez à cet article

Source : *BlueBorne : le hack qui permet de pirater un téléphone sans le toucher*

De Britney Spears aux ambassades, ESET livre ses recherches sur le groupe Turla

	De Britney Spears aux ambassades, ESET livre ses recherches sur le groupe Turla

Il y a quelques mois, le groupe de cybercriminels Turla utilisait le compte Instagram® de Britney Spears pour mener des campagnes de cyberespionnage. ESET® est le premier éditeur à identifier et documenter leur nouvelle backdoor, nommée Gazer, visant principalement des institutions européennes. ESET publie un document complet d'analyse.

Qui est le groupe Turla

Groupe de cybercriminels menant des campagnes d'espionnage depuis plusieurs années, il **cible principalement les gouvernements européens et les ambassades.** Turla est connu pour mener des attaques dites de « point d'eau » (surveiller les habitudes de navigation de la victime) et des campagnes de spearphishing (e-mails infectés ciblés).

Les chercheurs d'ESET ont découvert **la backdoor Gazer sur nombre d'ordinateurs à travers le monde, mais principalement en Europe.** « Les techniques employées sont similaires aux précédentes campagnes menées par le groupe : une première porte dérobée s'installe par spearphishing, puis une seconde backdoor est envoyée sur le poste compromis. Il s'agit ici de Gazer », explique Jean-Ian Boutin, senior Malware Researcher chez ESET.

Détecter l'indétectable

Comme d'autres backdoors « second stage » avant elle (telles que Carbon et Kazuar), Gazer reçoit ses tâches au format chiffré à partir d'un serveur C&C. Ce dernier peut être une machine déjà infectée ou n'importe quelle autre machine en réseau. Le Groupe Turla utilise ses propres moyens de chiffrement reposant sur 3DES et RSA. L'analyse des clés RSA montre qu'elles contiennent la clé publique du serveur contrôlée par l'attaquant et une clé privée. Pour chaque échantillon analysé, ESET a découvert que les clés utilisées sont uniques et que tous les échanges avec le C&C sont chiffrés.

Architecture de la backdoor Gazer

Pour échapper à la détection et assurer sa persistance, les chercheurs ESET ont découvert que la menace utilisait un système de fichier virtuel dans le registre Windows. « Turla va très loin pour éviter d'être repéré. Le groupe supprime tout d'abord ses fichiers des systèmes compromis, puis change les chaînes et les indicateurs de compromission pour chaque version de leur backdoor. On note un certain sens de l'humour des cybercriminels qui **utilisent des références à des jeux vidéo dans leur code.** », poursuit Jean-Ian Boutin.

Pour plus de détails concernant la nouvelle backdoor employée par Turla, consultez WeLiveSecurity ou notre livre blanc. Nous restons à votre disposition pour plus de renseignements.

Réagissez à cet article

Source : *Boîte de réception (570) – denis.jacopini@gmail.com – Gmail*

Les juges européens sanctionnent la surveillance des courriels privés au travail

Les juges européens sanctionnent la surveillance des courriels privés au travail

La Cour européenne des droits de l'homme (CEDH) a sanctionné l'utilisation de courriels privés dans le cadre d'un licenciement. Cette décision fera jurisprudence partout en Europe.

Jusqu'où un employeur peut-il aller dans la surveillance d'Internet? C'est à cette question que viennent de répondre – ce mardi – les 17 juges de la Grande Chambre, l'instance suprême de la Cour européenne des droits de l'homme (CEDH) de Strasbourg. Les juges européens ont sanctionné en appel la surveillance des courriels privés par un employeur en Roumanie qui avait licencié dans la foulée un de ses salariés – Bogdan Mihai Barbulescu – en 2007. Cette décision de la CEDH était très attendue car elle fera jurisprudence pour les 47 États membres du Conseil de l'Europe, dont les approches en la matière sont très différentes.

Lire aussi»Attention aux courriels personnels envoyés du bureau

Les juges, statuant en appel d'une décision de 2016, ont considéré que les autorités nationales roumaines n'avaient pas correctement protégé le droit de Bogdan Mihai Barbulescu au respect de sa vie privée et de sa correspondance et n'ont donc pas ménagé un juste équilibre entre les intérêts en jeu, précise la décision adoptée par 11 voix contre 6.

La CEDH avait été saisie par Bogdan Mihai Barbulescu, un ingénieur roumain de 38 ans. Son employeur l'avait licencié en 2007 après avoir constaté – en surveillant ses communications électroniques – qu'il avait utilisé la messagerie de la société à des fins personnelles, en infraction au règlement intérieur. L'ingénieur avait ensuite dénoncé l'espionnage de ses communications par son employeur, s'estimant victime d'une violation du droit au respect de la vie privée et de la correspondance protégée par l'article 8 de la convention européenne des droits de l'homme: cet article proclame le droit de toute personne au respect «de sa vie privée et familiale, de son domicile et de sa correspondance». Les tribunaux roumains avaient débouté Bogdan Mihai Barbulescu, jugeant que la conduite de l'employeur avait été raisonnable et que la surveillance des communications avait constitué le seul moyen d'établir qu'il y avait infraction disciplinaire. Une approche confirmée en janvier 2016 par la CEDH, qui avait validé la possibilité pour un employeur de surveiller l'usage de l'Internet dans sa société dans le cadre d'une procédure disciplinaire…[lire la suite]

Réagissez à cet article

Source : *Les juges européens sanctionnent la surveillance des*

courriels privés au travail